hw

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,015	09/27/2001	Vincent J. Zimmer	42390P11198	4663

7590 11/02/2005

Tom Van Zandt
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
PROCTOR, JASON SCOTT	
ART UNIT	PAPER NUMBER
2123	

DATE MAILED: 11/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/966,015	**Applicant(s)** ZIMMER, VINCENT J.	
	Examiner Jason Proctor	**Art Unit** 2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 October 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9,11,15,17,27,29,32 and 37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9,11,15,17,27,29,32 and 37* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 March 2005* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Claims 1-3, 7-9, 11, 15, 17, 21-27, 30-35, and 37 were rejected in Final Office Action dated 29 June 2005, while claims 28, 29, and 36 were objected to as allowable if written in independent form and rejections under 35 U.S.C. §§ 101 and 112 were overcome. Applicants' response dated 14 October 2005 has cancelled numerous claims and amended claims 9, 11, 15, 17, 27, 29, 32, and 37.

Claims 9, 11, 15, 17, 27, 29, 32, and 37 are currently pending in this application. The limitations presented by these claims are substantially compliant with the statement of allowable subject matter in the previous Office Action.

The indicated allowability of claims 28, 29, and 36 is withdrawn in view of the newly discovered reference(s) to Davis, US Patent No. 5,844,986. Rejections based on the newly cited reference(s) follow.

Claims 9, 11, 15, 17, 27, 29, 32, and 37 have been rejected.

Claim Objections

1. Claim 9 is objected to because of the following informalities: Claim 6 appears to omit a semicolon in line 6. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. § 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

2. Claims 9, 11, 15, 17, 32, are 37 rejected under 35 U.S.C. § 103(a) as being unpatentable over US Patent No. 6,397,242 to Devine et al. (Devine) in view of "Extensible Firmware Interface Specification Version 1.02" by Intel Corporation (Intel) and further in view of US Patent No. 5,844,986 to Davis (Davis).

As an initial matter, the Examiner observes that the publication date of the Intel reference is December 12, 2000, which qualifies it as prior art under 35 U.S.C. § 102(a), and therefore not subject to the exclusions of prior art under 35 U.S.C. § 103(c). The publication date of the Davis reference is December 1, 1998, which qualifies it as prior art under 35 U.S.C. § 102(b), and therefore not subject to the exclusions of prior art under 35 U.S.C. § 103(c).

Regarding claim 9, Devine discloses a system implementing a virtual machine monitor (VMM) upon a computer having a native environment that executes in physical mode [*“One solution that was the subject of intense research in the late 1960’s and 1970’s came to be known as the ‘virtual machine monitor’ (VMM)”* (column 1, lines 36-52); *“Virtual machine monitors can also provide architectural compatibility between different processor architectures by using a technique known as either ‘binary emulation’ or ‘binary translation’.”* (column 2, lines 21-35); *“The virtual machine 120 then will also include the virtual operating system (VOS) 700, which communicates with the “real,” or “physical” system hardware 710 via the VMM 100.”* (column 24, lines 39-51)].

Devine discloses emulating legacy hardware components that are not present in the native environment using the VMM to provide support for legacy code running on the computer system [*“Virtual machine monitors (VMM) have many attractive properties.* [...] *Furthermore, they allow modern operating systems to coexist, not just the legacy operating system that legacy virtual machine monitors allow.* (column 4, lines 23-36)].

Devine does not expressly teach that the VMM is “firmware-based”, however Devine does teach that the VMM does not require a host operating system [*“Fig. 8 is a block diagram that illustrates the fact that invention – switching between binary translation and direct execution modes – does not require a host operating system.”* (column 24, lines 60-67)]. The significance of a VMM that does not require a host operating system is explained by Applicants’ arguments (response dated 25 March 2005, page 12):

> Clearly, this conventional legacy VMM [taught by Bugnion] is not firmware-based, but rather runs on top of an existing operating system or is part of an existing operating system. This is significant because a software application used to access hardware runs significantly slower than firmware components used to access the same hardware since **the software application is layered on an operating system, which, in**

> **turn, is layered over a firmware layer sitting between the operating system and the hardware.** (emphasis added)

Devine expressly discloses a VMM corresponding to Applicants' arguments, that is, a VMM that does not require an operating system, which implicitly discloses a VMM that is not a software application, is not layered on an operating system, and which therefore resides at the firmware level directly on the hardware.

Devine does not expressly disclose implementing the VMM combined with an extensible firmware interface.

Intel discloses implementing an extensible firmware interface via which firmware modules are loaded during a pre-boot phase of the computer system [*"This Extensible Firmware Interface (hereafter known as EFI) Specification describes an interface between the operating system (OS) and the platform firmware.* [...] *The EFI specification is designed as a pure interface specification.* [...] *Similarly, the specification defines the set of interfaces and structures that the OS may use in booting."* (page 1, first and second paragraphs)].

Intel expressly suggests the addition of "OS-neutral platform value-add", specifically the creating of "platform drivers" that *"may be used to implement enhanced platform capabilities like* [...] *security*" (page 5, second paragraph).

Intel teaches several advantages of the EFI [*Using this formal definition, a shrink-wrap OS intended to run on Intel® architecture-based platforms will be able to boot on a variety of system designs without further platform or OS customization. The definition will also allow for platform innovation to introduce new features and functionality that enhance platform capability without requiring new code to be written in the OS boot sequence."* (page 1); *"Furthermore, an* *abstract specification opens a route to replace legacy devices and firmware code over time. New device types and associated code can provide equivalent functionally through the same defined abstract interface, again without impact on the OS boot support code."* (page 1)].

It would have been obvious to a person of ordinary skill in the art at the time of Applicants' invention to combine the invention of Devine, a VMM that virtualizes an architecture to enable execution of non-native operating systems, with the teachings of Intel regarding an extensible firmware framework. Motivation to do so would be found in the teachings of Intel, particularly to improve support for a non-native "shrink-wrap OS" on the computing system using the VMM taught by Devine. Both Devine and Intel are directed, at least in part, toward support for a non-native operating system on a particular architecture.

Devine in view of Intel does not explicitly disclose the limitations of authenticating firmware modules as recited by the claim.

Davis discloses authenticating a firmware module by comparing a digital signature provided with the firmware module with digital signatures stored in secure storage that is accessible to the authenticator [*"The authentication and validation are performed by a security processor which contains the BIOS firmware. One example of such a security processor is a cryptographic coprocessor. The cryptographic processor authenticates and validates the BIOS firmware by using secret information such as a digital signature embedded in the BIOS upgrade."* (column 2, lines 58-63)].

It would have been obvious to a person of ordinary skill in the art at the time of Applicants' invention to combine the firmware authenticating features of Davis with the combined invention of Devine in view of Intel at the explicit suggestion by Intel that EFI *"may be used to implement enhanced platform capabilities like* [...] *security*" (page 5, second paragraph). Davis clearly discloses a means of enhancing firmware security. The combination would be achieved by implementing Davis' disclosed "security processor" or its equivalent. It would have been obvious to a person of ordinary skill in the art that the VMM of Devine in view of Intel would act as the functional equivalent of Davis' "security processor" because the VMM is already acting in a supervisory role and accessing the EFI.

Claim 15 recites an apparatus corresponding to the method performed in claim 9 and is rejected for the same reasons given above regarding claim 9.

Regarding claim 11 and 17, Devine discloses that the VMM provides at least PC/AT hardware emulation [*"The invention is particularly well-suited for virtualizing computer systems in which the hardware processor has an Intel x86 architecture that is compatible with at least the Intel 80386 processor."* (column 6, lines 53-56)].

Regarding claim 32, the generation and use of log files in the computer system arts is old and well known. Microsoft Computer Dictionary, Fifth Edition, provides *log*, "A record of transactions or activities that take place on a computer system". It would have been obvious to a person of ordinary skill in the art to implement the well-known concept of a log in order to track and identify which firmware modules have been loaded and authenticated.

Regarding claim 37, Intel expressly discloses enabling a legacy option ROM to run and effect its input/output services ["*The PC industry has a huge investment in Intel Architecture Option ROM technology, and the obsolescence of this installed base of technology is not practical in the first generation of EFI-compliant system. The interfaces have been designed in such as way* [sic] *as to map back into legacy interfaces. These interfaces have in no way been burdened with any restrictions inherent to legacy Option ROMs.*" (page 14)].

Regarding the limitation of "translating the results of the I/O services into a native API," the disclosure of the instant application states (paragraph 0014):

> The VMM then translates the results [of the legacy option ROM running and effecting its I/O services] into a native API. That is, the VMM traps the I/O to the semantic equivalent in the native environment.

In a VMM that supports emulation of a non-native architecture, this is regarded as an inherent feature. Failure to perform this function would render the legacy option ROM inoperable in combination with the VMM. Therefore this limitation is an obvious detail of implementation of when combining support for a legacy option ROM with the invention of Devine.

3. Claims 27 and 29 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Devine in view of Davis.

Devine teaches that the VMM does not require a host operating system [*"Fig. 8 is a block diagram that illustrates the fact that invention – switching between binary translation and direct execution modes – does not require a host operating system."* (column 24, lines 60-67)]. The significance of a VMM that does not require a host operating system is explained by Applicants' arguments (response dated 25 March 2005, page 12):

> Clearly, this conventional legacy VMM [taught by Bugnion] is not firmware-based, but rather runs on top of an existing operating system or is part of an existing operating system. This is significant because a software application used to access hardware runs significantly slower than firmware components used to access the same hardware since **the software application is layered on an operating system, which, in turn, is layered over a firmware layer sitting between the operating system and the hardware.** (emphasis added)

Devine expressly discloses a VMM corresponding to Applicants' arguments, that is, a VMM that does not require an operating system, which implicitly discloses a VMM that is not a software application, is not layered on an operating system, and which therefore resides at the firmware level directly on the hardware. Devine's VMM is therefore implemented to execute during the pre-boot phase of the computer system.

Devine does not explicitly disclose the limitations of authenticating firmware modules as recited by the claim.

Davis discloses authenticating a firmware module by comparing a digital signature provided with the firmware module with digital signatures stored in secure storage that is accessible to the authenticator [*"The authentication and validation are performed by a security processor which contains the BIOS firmware. One example of such a security processor is a cryptographic coprocessor. The cryptographic processor authenticates and validates the BIOS firmware by using secret information such as a digital signature embedded in the BIOS upgrade."* (column 2, lines 58-63)].

It would have been obvious to a person of ordinary skill in the art at the time of Applicants' invention to combine the authentication features taught by Davis with the VMM of Devine in order to provide legacy hardware support on a secure computer platform. Devine expressly teaches the use of a VMM for legacy hardware support (column 4, lines 23-36) while

Davis expressly teaches the advantages of authenticating firmware (column 1, lines 46-62), and the advantages of a secure computer platform are well known to persons of ordinary skill in the art. The combination would be achieved by implementing Davis' disclosed "security processor" or its equivalent. It would have been obvious to a person of ordinary skill in the art that the VMM of Devine would act as the functional equivalent of Davis' "security processor" because the VMM is already acting in a supervisory role by virtualizing the hardware.

Regarding claim 29, the generation and use of log files in the computer system arts is old and well known. Microsoft Computer Dictionary, Fifth Edition, provides *log*, "A record of transactions or activities that take place on a computer system". It would have been obvious to a person of ordinary skill in the art to implement the well-known concept of a log in order to track and identify which firmware modules have been loaded and authenticated.

Conclusion

Art considered pertinent by the examiner but not applied has been cited on form PTO-892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason Proctor whose telephone number is (571) 272-3713. The examiner can normally be reached on 8:30 am-4:30 pm M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Leo Picard can be reached at (571) 272-3749. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application should be directed to the TC 2100 Group receptionist: 571-272-2100. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Proctor
Examiner
Art Unit 2123

jsp

Paul L. Rodriguez 10/28/05
Primary Examiner
Art Unit 2125